Configuring Avaya Aura® Solution for Midsize Enterprise with the Communication Server 1000

Release 6.1
Issue 1
April 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

Avaya Aura® is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Introduction to CS 1000 configuration....7
- Before you begin....7
- Tracking values....7

Chapter 2: Avaya Aura® configuration....9
- Defining a SIP entity....9
- Creating entity links....9
- Adding routing policies....10
- Adding dial patterns....11

Chapter 3: CS 1000 configuration....13
- Launching Unified Communications Manager....13
- Obtaining node ID and IP addresses....14
- Administering ISDN....15
- Administering a virtual D-channel....15
- Administering zones....16
- Virtual SIP routes and trunk administration....17
 - Administering SIP routes and trunks....17
 - Administering virtual trunk routes....18
 - Administering ISDN routes....18
 - Administering trunks....19
 - Administering route list block....20
 - Administering a distant steering code....20
- Node SIP parameters administration....21
 - Administering codecs....21
 - Administering gateways....22
 - Administering gateway settings....23
 - Synchronizing configuration files....24
- Launching NRS Manager....24
- Administering a service domain....25
- SIP gateway endpoint administration....27
 - Administering a gateway endpoint for Session Manager....27
 - Administering a gateway endpoint for the redirect server....28
- Administering routing entries....29
- Cutting over and committing changes....30

Index....31

Chapter 1: Introduction to CS 1000 configuration

This document provides a sample configuration of a SIP trunk network that uses an Avaya Aura® Solution for Midsize Enterprise connected to an Avaya Aura® Communication Manager and an Avaya Communication Server 1000 (formerly Nortel). This sample configuration also uses Avaya 96*xx* SIP telephones as endpoints.

Before you begin

You must install and configure an Avaya Aura® Midsize Enterprise system before you can configure the Midsize Enterprise to work with Avaya Communication Server 1000. Make sure you read and complete the tasks in the following documents before you start on the tasks in this document:

- *Overview of Avaya Aura® Solution for Midsize Enterprise*
- *Installing and Configuring Avaya Aura®Solution for Midsize Enterprise*
- *Installing the Avaya S8800 Server for Avaya Aura® Solution for Midsize Enterprise*

Tracking values

Print or detach this page in order to keep track of the values you need to remember. You need to use all of the following values more than once. Make sure you write down these values after you administer them.

Node ID
Node IP address
TLAN IP address
D-channel number
Bandwidth zone number
Route number
Route list block number

Gateway password (optional)

Chapter 2: Avaya Aura® configuration

Defining a SIP entity

Use this procedure to add the Avaya Communication Server 1000 as a SIP entity.

1. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. Under **SIP Entity Details**, go to the **Name** field and enter a name for the SIP entity.
 Example: `CS1000-Node_Server`
4. In the **FQDN or IP Address** field, enter the IP address of the TLAN node.
5. If you need to specify a location for the SIP entity, go to the **Location** drop-down menu and select the appropriate location.
6. From the **Time Zone** drop-down menu, select the appropriate time zone.
7. From the **SIP Link Monitoring** drop-down menu, select **Link Monitoring Enabled**.
8. Click **Commit**.

Next steps

Continue to Creating entity links on page 9.

Creating entity links

Prerequisites

Defining a SIP entity on page 9

An entity link is a SIP trunk between Session Manager and a telephony system, in this case a Avaya Communication Server 1000. Use this procedure to add entity links.

1. From the left of the SIP Entity Details screen, select **Entity Links**.
2. Click **New**.
3. On the new row, enter a name for the new SIP entity in the **Name** field.
 Example: `ASM1-to-S8800`
4. From the **SIP Entity 1** drop-down menu, select the Session Manager name.
 SIP Entity 1 must always be a Session Manager instance.
5. In the **Port** field, enter the port number where the other system *sends* SIP requests.
 The default port for TCP and UDP is 5060. The default port for TLS is 5061.
6. From the **SIP Entity 2** drop-down menu, select the name of the other system.
7. In the next **Port** field, enter the port number where the other system *receives* SIP requests.
 Example: 5060
8. Check the **Trusted** box.
 If this box is *not* checked, calls from the associated SIP entity are denied.
9. Click **Commit**.
10. Repeat this procedure to add an entity link for the Avaya Communication Server 1000.

Next steps

Continue to Adding routing policies on page 10.

Adding routing policies

Prerequisites

Creating entity links on page 9

Use this procedure to add a routing policy for the CS 1000.

Routing policies describe the conditions under which calls are routed to the SIP entities. You need to add a routing policy only for the CS 1000. Since the SIP 96*xx* endpoints are registered on Session Manager, you do not need to define a routing policy for Communication Manager. The necessary SIP communication between Session Manager and Communication Manager was previously administered along with the sequenced application.

1. On the left pane of the System Manager console, navigate to **Network Routing Policy** > **Routing Policies**.
2. Click **New**.
3. Under **General** on the Routing Policy Details screen, go to the **Name** field and enter a descriptive name for the routing policy.
 Example: Chicago CS 1000
4. Under **SIP Entity as Destination**, click **Select**.
5. Select the appropriate SIP entity to which this routing policy applies.
6. Keep the default settings for the remaining fields.
7. Click **Commit** to save each routing policy definition.

Next steps

Continue to Adding dial patterns on page 11.

Adding dial patterns

Prerequisites

Adding routing policies on page 10

Use this procedure to define dial patterns that direct calls to the appropriate SIP entity. In the provided examples, calls are routed to the CS 1000 using seven-digit extensions beginning with 777.

1. On the left side of the System Manager console, navigate to **Network Routing Policy** > **Dial Patterns**.
2. Click **New**.
3. On the Dial Pattern Details screen, go to the **Pattern** field and enter the dialed number or prefix.
 Example: 777
4. In the **Min** field, enter the minimum length of the dialed number.
 Example: 7
5. In the **Max** field, enter the maximum length of the dialed number.
 Example: 7
6. In the **SIP Domain** drop-down list, select the appropriate SIP domain or **ALL**.

7. In the **Notes** field, enter a string describing the purpose of dial pattern. Example: IP phones on Chicago CS 1000
8. Under **Originating Locations and Routing Policies**, click **Add**.
9. From the list choose one of the following options:
 - The appropriate location or **ALL**
 - The appropriate routing policy
10. Keep the default settings on the remaining fields.
11. Click **Commit** to save the dial pattern.

Chapter 3: CS 1000 configuration

The Avaya Avaya Communication Server 1000 uses the Network Routing Server (NRS) to provide SIP and H.323 signaling interfaces to IP networks. The NRS communicates with the CS 1000 call server over a private ethernet interface. There can be one or more NRS-supported CS 1000 instances. The applications that can run on the NRS include:

SIP Signaling Gateway (SSG): Provides SIP signaling for IP networks.

H.323 Gateway: Provides H323 Redirect & Registrar service components.

NRS Manager: Provides a Web interface for NRS management.

Element Manager: Provides a Web interface for system administrative tasks.

The procedures in this section assume that you have:

- A CS 1000 with one NRS and call server co-resident on the same CS 1000 server blade
- An Element Manager Web interface to configure system resources such as SIP virtual routes and trunks
- An NRS Manager to configure the routing for SIP devices
- A Coordinated Dial Plan (CDP) feature to route calls from the CS 1000 over the SIP trunks to Session Manager to reach the 96*xx* endpoints registered to Session Manager

Launching Unified Communications Manager

If you have a Avaya Communication Server 1000 7.5, you can have UCM hosted on the System Manager or located with the Linux system elements.

1. Using your browser, access the CS 1000 using the FQDN or TLAN IP address of the UCM server.
 Example: `https://10.80.51.20`
2. Log in with the appropriate user name and password.
3. From the Unified Communications Management screen, select the appropriate CS 1000 **Element Name** and **Element Type**.

Next steps

Continue to Obtaining node ID and IP addresses on page 14.

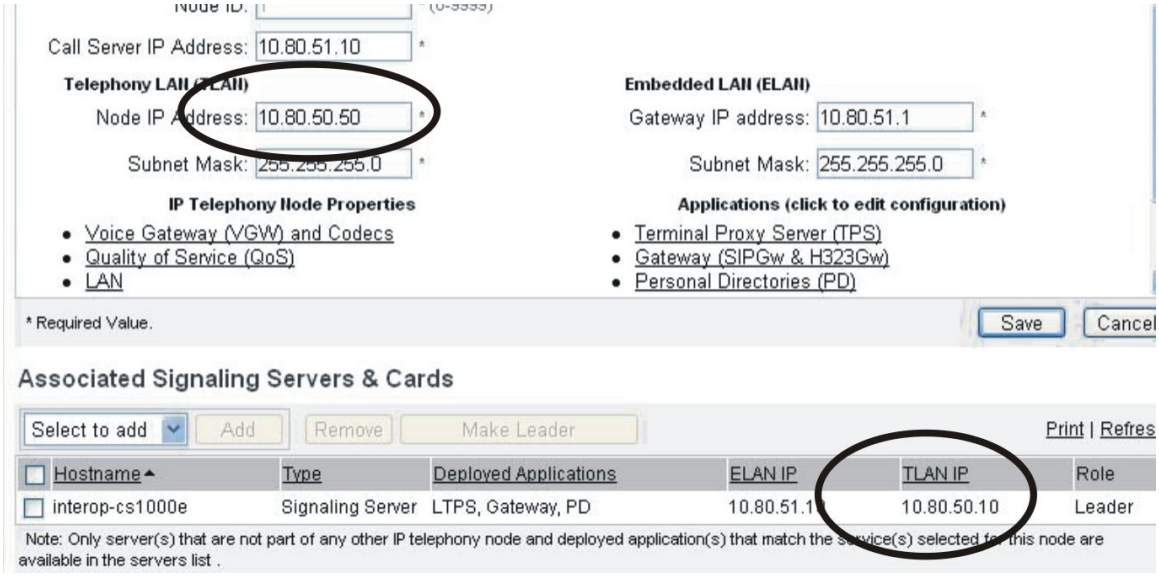
Obtaining node ID and IP addresses

Prerequisites

Launching Unified Communications Manager on page 13

1. From the Element Manager, navigate to **System** > **IP Network** > **Nodes: Servers, Media Cards**.
2. From the **IP Telephony Nodes** screen, select the appropriate **Node ID** row to expand it.

 Important:
 Write down this **Node ID** because you will need it for several subsequent procedures.
3. When the screen updates with additional information, note the values in the **Node IP Address** and the signaling server **TLAN IP** fields. You need these values to configure subsequent sections.



Next steps

Continue to Administering ISDN on page 15.

Administering ISDN

Prerequisites

Obtaining node ID and IP addresses on page 14

1. From the left pane of the Element Manager, select **Customers**.
2. Under **Customers**, select the link associated with the appropriate customer.

 Note:
 The system can support more than one customer with different network settings and options.
3. Under **Customer *XX* Property Configuration**, select **Feature Packages**.
4. When the screen updates, select **Integrated Services Digital Network**.
5. Under **Integrated Services Digital Network**, select the **Integrated Services Digital Network (ISDN)** check box.
6. Keep the default values for the remaining fields.
7. Scroll to the bottom of the screen and click **Save**.

Next steps

Continue to Administering a virtual D-channel on page 15.

Administering a virtual D-channel

Prerequisites

Administering ISDN on page 15

1. From the left pane of the Element Manager, navigate to **Routes and Trunks** > **D-Channels**.
2. Under **D-Channels**, go to the **Choose a D-Channel Number** drop-down list and select an available D-channel.
 Example: 1

3. Write down this number because you will need it to administer ISDN routes in a subsequent procedure.
4. Click **to Add**.
5. Under **D-Channels *X* Property Configuration**, go to the **D channel Card Type (CTYP)** drop-down menu and select **D-Channel is over IP (DCIP)**.
6. In the **Designator (DES)** field, enter a descriptive name for the D-channel.
 Example: SIPtoASM
7. Keep the default values for the remaining fields.
8. Click **Submit**.

Next steps

Continue to Administering zones on page 16.

Administering zones

Prerequisites

Administering a virtual D-channel on page 15

1. From the left pane of the Element Manager, navigate to **IP Network** > **Zones** > **Bandwidth Zones**.
2. Under **Bandwidth Zones**, go to the **Please Choose the** drop-down list and select an available zone number.
 Example: **Bandwidth Zones 3**
3. Write down this bandwidth zone number because you will use it to administer virtual trunk routes in a subsequent procedure.
4. Click **to Add**.
5. Under **Zone Basic Property and Bandwidth Management**, go to the **Zone Intent (ZBRN)** drop-down menu and select **VTRK (VTRK)**.
6. In the **Description (ZDES)** field, enter a descriptive name for the zone.
 Example: ASMSIPZONE
7. Keep the default values for the remaining fields.
8. Click **Submit**.

Next steps

Continue to the procedures under Virtual SIP routes and trunk administration on page 17.

Virtual SIP routes and trunk administration

Administering SIP routes and trunks

Prerequisites

Administering zones on page 16

1. Starting from the left pane of the Element Manager, navigate to **Routes and Trunks** > **Routes and Trunks** .
2. Under **Routes and Trunks**, go to the applicable **Customer** row and click **Add route**.
3. Under **Customer *X*, Route *X* Configuration**, go to the **Route Number (ROUT)** field and enter an available route number.
 Example: 1
4. Write down the route number you used because you will need it to administer the route list block.
5. In the **Designator field for trunk (DES)** field, enter a description of the trunk.
 Example: SIPNRS
6. In the **Trunk Type (TKTP)** field, enter `TIE` for the TIE trunk data block.
7. From the **Incoming and outgoing trunk (ICOG)** drop-down menu, select **Incoming and Outgoing (IAO)**.
8. In the **Access code for the trunk route (ACOD)** field, enter an available access code.
 Example: 7770001
9. Keep the default values for the remaining fields.

Next steps

Leave this screen open and continue to Administering virtual trunk routes on page 18.

Administering virtual trunk routes

Prerequisites

Administering SIP routes and trunks on page 17

1. On **Routes and Trunks**, scroll down the screen and check **The route is for a virtual trunk route (VTRK)**.
 Four additional fields display.
2. In the **Zone for codec selection and bandwidth management (ZONE)** field, enter the bandwidth zone number you wrote down when you administered zones.
 Example: 3
3. In the **Node ID of signaling server of this route (NODE)** field, enter the node ID you wrote down when you obtained node and IP addresses.
 Example: 1
4. From the **Protocol ID for the route (PCID)** drop-down menu, select **SIP (SIP)**.

Next steps

Leave this screen open and continue to Administering ISDN routes on page 18.

Administering ISDN routes

Prerequisites

Administering virtual trunk routes on page 18

1. On **Routes and Trunks**, scroll down the screen and check **Integrated Services Digital Network option (ISDN)**.
 Six additional fields display.
2. From the **Mode of operation (MODE)** drop-down menu, select **Route uses ISDN Signaling Link (ISLD)**.
3. In the **D channel number (DCH)** field, enter the D-channel number you wrote down when you administered virtual D-channels.
 Example: 1
4. In the **Private network identifier (PNI)** field, set the PNI to a number between 1 and 32700.
5. Check the **Network calling name allowed (NCNA)** field.

6. Check the **Network call redirection (NCRD)** field.
7. Keep the default values for the remaining fields.
8. Click **Submit**.

Next steps

Leave this screen open and continue to Administering trunks on page 19.

Administering trunks

Prerequisites

Administering ISDN routes on page 18

You can use the **Multiple trunk input number (MTINPUT)** field to add multiple trunks in a single operation or to repeat the operation for each trunk.

1. On the refreshed **Routes and Trunks**, click **Add trunk** next to the newly-added route.
2. From **Customer *X*, Route *X*, New Trunk Configuration**, go to the **Trunk data block (TYPE)** drop-down menu and select **IP Trunk (IPTI)**.
3. In the **Terminal Number (TN)** field, enter an available terminal number.
 Example: 09600000
4. In the **Designator field for trunk (DES)** field, enter a description for the trunk.
 Example: ASMSIPTRK
5. In the **Extended Trunk (XTRK)** field, enter `VTRK` for the virtual trunk.
6. In the **Route number, Member number (RTMB)** field, enter a current route number and starting member number.
 Example: 11
7. From the **Card Density (CDEN)** drop-down menu, select **Octal Density (8D)**.
8. From the **Start arrangement Incoming (STRI)** drop-down menu, select **Wink or Fast Flash (WNK)**.
9. From the **Start arrangement Outgoing (STRO)** drop-down menu, select **Wink or Fast Flash (WNK)**.
10. In the **Trunk Group Access Restriction (TGAR)** field, enter the appropriate trunk group access restriction level.
 Example: 1
11. In the **Channel ID for this trunk (CHID)** field, enter an available starting channel ID.

Example: 1

12. Keep the default values for the remaining fields.
13. Scroll to the bottom of the screen and click **Save**.

Next steps

Continue to Administering route list block on page 20.

Administering route list block

Prerequisites

Administering trunks on page 19

1. From the left pane of the Element Manager, navigate to **Dialing and Numbering Plans** > **Electronic Switched Network**.
2. Under **Electronic Switched Network (ESN)**, select **Route List Block (RLB)**.
3. Under **Route List Blocks**, go to the **Please enter a route list index** field and enter an available route list block number.
 Example: 1
4. Write down the route list block number you used because you will need it to administer the distant steering code.
5. Click **to Add**.
6. Under **Route List Block**, go to the **Route Number (ROUT)** field and select the route number you used when you administered the SIP routes and trunks.
 Example: 1
7. Keep the default values for the remaining fields.
8. Scroll down to the bottom of the screen and click **Submit**.

Next steps

Keep this screen open and continue to Administering a distant steering code on page 20.

Administering a distant steering code

Prerequisites

Administering route list block on page 20

1. Under **Electronic Switched Network (ESN)**, select **Distant Steering Code (DSC)**.
2. Under **Distant Steering Code List**, go to the **Please enter a distant steering code** field and enter the dialed prefix digit you want matched.
 Example: `666`

 This would add an entry to route 666xxxx calls to Session Manager.
3. Click **to Add**.
4. Under **Distant Steering Code**, go to the **Route List to be accessed for trunk steering code (RLI)** drop-down menu and select the route list block number you created when you administered the route list block.
 Example: 1
5. Keep the default values for the remaining fields.
6. Click **Submit**.

Next steps

Continue to the procedures under Node SIP parameters administration on page 21.

Node SIP parameters administration

This section assumes that the TLAN and ELAN IP addresses have already been configured as a result of the basic signaling server configuration.

Related topics:

Administering codecs on page 21
Administering gateways on page 22
Administering gateway settings on page 23
Synchronizing configuration files on page 24

Administering codecs

Prerequisites

Administering a distant steering code on page 20

1. From the left pane of the Element Manager, navigate to **IP Network** > **Nodes: Servers, Media Cards** > **Configuration**.
2. Under **IP Telephony Nodes**, select the node ID of this CS 1000.
 This is the node ID you wrote down when you obtained the node ID and IP addresses.
3. Under **Node Details**, click **Voice Gateway (VGW) and Codecs**.

 Note:
 This procedure assumes that the TLAN and ELAN IP addresses were configured with the signaling server.
4. Under **General**, verify all the default values.
5. Scroll down and check the codecs you want enabled for your system.

 Note:
 Codec G.711 is checked by default and cannot be unchecked.
6. Click **Save**.

Next steps

Continue to Administering gateways on page 22.

Administering gateways

Prerequisites

Administering codecs on page 21

1. Under **Node Details**, click **Gateway (SIPGw and H.323Gw)**.
2. Under **Node ID: *X* – Virtual Trunk Gateway Configuration Details**, go to the **Vtrk Gateway Application** drop-down menu and select one of the following options, depending on what protocols are supported on your system:
 - **SIP Gateway (SIPGw)**
 - **SIPGw and H.323Gw**
3. In the **SIP Domain Name** field, enter the domain name you are using for this system.
 Example: avaya.com
4. In the **Local SIP Port** field, enter `5060`

5. In the **Gateway endpoint name** field, enter an appropriate name for the gateway.
 Example: CS1KGateway
6. Optional. In the **Gateway password** field, enter a password.

 You need a password only when the SSG is configured as a SIP Proxy and when registration is required. You do not need a password when the SSG is configured as a SIP redirect server.
7. If you set up a password, write it down because you will need it in a subsequent procedure.
8. Keep the default values for the remaining fields.
9. Click **Save**.

Next steps

Continue to Administering gateway settings on page 23.

Administering gateway settings

Prerequisites

Administering gateways on page 22

1. Click **SIP Gateway Settings**.
2. Under the **Proxy or Redirect Server** section, go to the **Primary TLAN IP Address** field and enter the TLAN IP address you wrote down when you obtained the node ID and IP addresses.
3. In the **Port** field, enter `5060`
4. From the **Transport Protocol** drop-down menu, select **TCP**.
5. For the **Options** under **Primary TLAN IP Address**, check **Support registration**.
6. Scroll down to the **SIP URI Map** section.
7. Under **Public E.164 Domain Names**, enter the appropriate **National** value for the network configuration.
 Example: `+1` (1 is the country code)
8. Enter the appropriate **Subscriber** value for the network configuration.
 Example: `+1732` (732 is the area code)

9. Keep the default values for the remaining fields.
10. Click **Save**.

Next steps

Continue to Synchronizing configuration files on page 24.

Synchronizing configuration files

Prerequisites

Administering gateway settings on page 23

1. Navigate to **IP Network** > **Nodes: Servers, Media Cards**.
2. Under **Node Details**, click **Save**.
3. Under **Node Saved**, click **Transfer Now...**.
4. Under **Synchronize Configuration Files**, select the appropriate signaling server and click **Start Sync**.
5. When the synchronization completes, click **Restart Applications**.

Next steps

Continue to Launching NRS Manager on page 24.

Launching NRS Manager

Prerequisites

Synchronizing configuration files on page 24

This procedure assumes that SIP communication between the CS 1000 and Session Manager uses TCP. This procedure also enables UDP at a global level, although it is possible to configure individual endpoints to use only TCP.

1. From the left pane of the Element Manager, select **UCM Network Services**.
2. From the UNIFIED COMMUNICATIONS MANAGEMENT screen, check the row whose **Element Type** displays **Network Routing Service**.
3. From the NETWORK ROUTING SERVICE MANAGER screen, click **Edit**.
4. Under **SIP Server Settings**, check the **UDP Transport enabled** field.
5. In the **Primary Server UDP IP** field, enter the node IP address you wrote down when you obtained the node ID and IP addresses in a previous procedure.
6. In the **Primary Server UDP port** field, enter `5060`
7. Check the **TCP Transport enabled** field.
8. In the **Primary Server TCP IP** field, enter the node IP address you wrote down when you obtained the node ID and IP addresses in a previous procedure.
9. In the **Primary Server TCP port** field, enter `5060`
10. Keep the default values for the remaining fields.
11. Click **Save**.

Next steps

Continue to Administering a service domain on page 25.

Administering a service domain

Prerequisites

Launching NRS Manager on page 24

The NRS hosts an active and a standby database. The active database is used for runtime queries, and the standby database is used for administrative modifications.

1. From the left pane of the NRS Manager, select **Domains**.
2. Next to **Managing**, select **Standby database** to switch to the standby database.
3. Click **Add**.
4. Under **Add Service Domain**, go to the **Domain name** field and enter the domain name you have been using in previous procedures.
 Example: avaya.com

5. In the **Domain description** field, enter a description of the domain.
 Example: ASMSIP
6. Click **Save**.
7. Select the **L1 Domains (UDP)** tab.
8. From the **Filter by Domain** drop-down menu, select the service domain you previously created.
 Example: avaya.com
9. Click **Add**.
 This step adds a new L1 domain.
10. Under **Add L1 Domain (*[domain name]*)**, enter the appropriate values for your network configuration in the following fields:

 Important:
 The following values are only examples.

Field	Example values
Domain name	`udp`
Domain description	`avaya udp domain`
E.164 country code	`1`
E.164 area code	`303`

11. Keep the default values for the remaining fields.
12. Click **Save**.
13. Select the **L0 Domains (CDP)** tab.
14. From the **Filter by Domain** drop-down menu, select your service domain.
 Example: avaya.com
15. From the adjacent drop-down menu, select **udp**, and click **Add**.
 This adds a new L0 domain.
16. Under **Add L0 Domain (*[domain name]* / udp)**, enter the appropriate values for your network configuration in the following fields:

 Important:
 The following values are only examples.

Field	Example values
Domain name	`cdp`
Domain description	`cs1000 L0 domain`

17. Keep the default values for the remaining fields.
18. Click **Save**.

Next steps

Continue to the procedures under SIP gateway endpoint administration on page 27.

SIP gateway endpoint administration

You need to configure two SIP gateway endpoints — one for the Session Manager server and the other for the SIP redirect server.

Related topics:

Administering a gateway endpoint for Session Manager on page 27
Administering a gateway endpoint for the redirect server on page 28

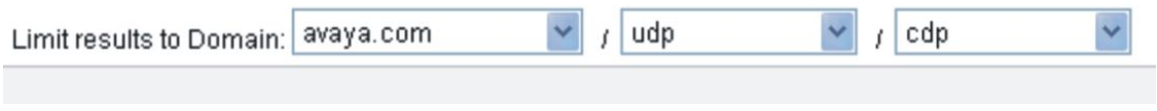
Administering a gateway endpoint for Session Manager

Prerequisites

Administering a service domain on page 25

Use this procedure to administer a gateway endpoint for the Session Manager server.

1. From the left pane of the NRS Manager, navigate to **Numbering Plans** > **Endpoints**.
2. Under **Search for Endpoints**, go to the **Limit results to Domain** drop-down menu and select your service domain followed by **udp** and **cdp**.
 Example:



3. Click **Add...**.
4. Under **Edit Gateway Endpoint (*[domain name]* / udp / cdp)**, enter the appropriate values for your network configuration in the following fields.

Important:
The values provided in these fields are only examples.

Field	Example values
End point name	ASM
Description	AvayaASM Chicago
E.164 country code	1
E.164 area code	905

5. Scroll down to the **Static endpoint address** field and enter the IP address of the Avaya Aura® Session Manager SM-100 Module interface.
6. Select the indicated values from the following drop-down menus.

Drop-down menu	Value
H.323 Support	**Not RAS H.323 endpoint**
SIP support	**Static SIP endpoint**

7. Check the box next to the **SIP TCP transport enabled** field.
8. Keep the default values for the remaining fields.
9. Click **Save**.

Next steps

Continue to Administering a gateway endpoint for the redirect server on page 28.

Administering a gateway endpoint for the redirect server

Prerequisites

Administering a gateway endpoint for Session Manager on page 27

Use this procedure to administer a gateway endpoint for the (formerly Nortel) redirect server.

1. Under **Edit Gateway Endpoint (*[domain name]* / udp / cdp)**, go to the **Endpoint authentication enabled** drop-down menu and choose to either enable or disable endpoint authentication, depending on your business requirements.
2. If you enabled endpoint authentication and you set up a password when you administered the gateway, go to the **Authentication password** field and use the same password.
3. Scroll down and in the **SIP support** drop-down menu, select **Dynamic SIP endpoint**.
4. Check the box next to the **SIP TCP transport enabled** field.
5. Keep the default values for the remaining fields.
6. Click **Save**.

Next steps

Continue to Administering routing entries on page 29.

Administering routing entries

Prerequisites

Administering a gateway endpoint for the redirect server on page 28

Use this procedure to administer two routing entries. The first entry uses the Session Manager gateway endpoint to reach the 96*xx* endpoints with extension digits 666*xxxx*. The second entry uses the redirect server gateway endpoint to reach endpoints with extension digits 777*xxxx*. These extension digits are used only as examples. Use the digits required for your system.

1. From the left pane of the NRS Manager, navigate to **Numbering Plans** > **Routes**.
2. Under **Search for Routing Entries**, go to the drop-down menus adjacent to **Limit results to Domain** and enter your service domain, **udp**, and **cdp**.
3. From the **Endpoint name** drop-down menu, select the endpoint name that corresponds to Session Manager.
 Example: ASM-BR-SIL
4. Click **Add…**.
5. Under **Add Routing Entry (*[domain name]* / udp / cdp / ASM)**, select the indicated values from the following drop-down menus and fields.

Drop-down menu	Value
DN type	**Private level 0 regional (CDP steering code)**
DN prefix	`666`
Route cost (1 – 255)	Enter an appropriate cost value.

6. Keep the default values for the remaining fields.
7. Click **Save**.
8. Repeat these steps to add a routing entry that reaches the CS 1000 endpoints behind the SIP redirect server gateway endpoint. These steps contain the following differences:
 - From the **Endpoint name** drop-down menu, select the endpoint name that corresponds to CS 1000. Example: CS1KGateway.
 - In the **DN prefix** field, enter `777`

Next steps

Continue to Cutting over and committing changes on page 30.

Cutting over and committing changes

Prerequisites

Administering routing entries on page 29

1. From the left pane of the NRS Manager, navigate to **System** > **Database**.
2. Click **Cut over**.
 The **Database status** changes to `Switched over` and the **Commit** button is enabled.
3. Click **Commit**.

Index

B

bandwidth zones 16

C

codecs 21
configuration files, synchronization 24
Coordinated Dial Plan (CDP) 13

D

D-channel 15
dial patterns 11
distant steering code 20

E

Element Manager 13
entity links 9

G

gateway endpoints
 redirect server 28
 Session Manager 27
gateway settings 23
gateways 22

H

H.323 Gateway 13

I

IP address 14
ISDN 15
ISDN routes 18

N

Network Routing Server (NRS) 13
node ID 14
NRS Manager 13, 24

R

redirect server gateway endpoints 28
route list block 20
routing entries 29
routing policies 10

S

service domain 25
Session Manager
 gateway endpoints 27
SIP entity 9
SIP routes 17
SIP Signaling Gateway (SSG) 13

T

TLAN IP address 14
trunk routes 18
trunks 17, 19

U

Unified Communications Manager 13

V

virtual D-channel 15
virtual trunk routes 18

Z

zones 16